REMARKS:

Claims 156 and 158-191 were pending in the application. Claims 156, 159-162, 164-170, 172-175, 177-182, 184-187, 189-191 have been amended. Therefore, claims 156 and 158-191 remain pending in this application.

Section 103 Rejections

The Examiner rejected all of the pending independent claims under 35 U.S.C. § 103 based on Shear (U.S. Patent 4,827,508 A) in view of Matyas, Jr. et al. (U.S. Patent 4,850,017), Sklut et al. (U.S. Patent 5,270,773), and Narasimhalu et al. (U.S. Patent 5,499,298). As noted below, Applicants submit that the present claims are patentably distinct over the cited references.

Shear (U.S. Patent 4,827,508)

Shear describes a system that meters the usage of proprietary data encrypted in a database. Shear Abstract, lines 1-6. As Shear explains: "With the present invention, a CD-ROM disk, for example, might contain [a database of] all issues of 10 separate publications," *id.* at col. 4 lines 9-13, and "a user will be able to pay … according to his usage of the product". *Id.* at col. 6, lines 13-15. Shear's device enables "permit[ted] users to access and manipulate" this information locally "using their own computer equipment." *Id.* at col. 2 lines 29-35.

Matyas, Jr. et al. (U.S. Patent 4,850,017)

Matyas is concerned with generating a cryptographic key at one location and "*controlling the use of [the] cryptographic key*" at another location. Matyas, abstract, lines 1-3 (emphasis added). For example, if Matyas generated a key to be used only for encryption purposes, a user of the key would not be allowed to decrypt with the key. *Id.* at col. 7, lines 60-65. To guarantee that a cryptographic key is used as intended, Matyas associates a "control value" with the key that "specif[ies] the use" and "is transmitted" with the key. When a user desires to perform an action with the key, Matyas requires the user to provide the key and control value to a function that "ensure[s] that a requested key and control value are valid before allowing the key to be used." *Id.* at col. 7, lines 64 to col. 8, lines 1.

Sklut et al. (U.S. Patent 5,270,773)

Sklut relates generally to "[a]n image producing device such as a copier or printer." *See* Sklut Abstract. More particularly, Sklut addresses the issue of purging sensitive documents from a paper path that are left from a previous job (e.g. clearing a paper jam). Sklut col. 1, lines 32-43. When such an event occurs, Sklut teaches restricting access to the purging the device. *Id.* at col. 4, lines 10-12.

For example, Sklut describes "covering the entire paper path" with "locked access panels," and "hav[ing] unique keys to access [their] inner paper path components." *Id.* at col. 4, line 65 to col. 5, line 1. **Applicant submits that this reference to "key" in Sklut (and every other reference) is not to a "utilization permit" key (e.g. as in claim 156), but rather to a physical key that is used to open a lock and gain physical access to some portion of the device.**

Narasimhalu et al. (U.S. Patent 5,499,298)

Narasimahlu discloses "a method and apparatus for controlling the dissemination of digital information." Narasimahlu, abstract. To accomplish this task, Narasimahlu describes a packet structure that contains a control header and an encrypted body of data. *Id.* at col. 5 lines 35-37 and Fig. 2.

Narasimahlu's header contains several parameters that are used to control the number of times and when the body of data can be accessed. Examples of these parameters include "an access window 37 (AW), total number of legal accesses allowed 38 (TAL), the number of legal accesses left 39 (LAL)." Narasimahlu col. 5, lines 43-47. As Narasimahlu explains, the access window is "a specified time period in which a legal access is granted" and contains "[a] start and end time [that] is given as the boundary." *Id.* at col. 5 lines 56-60. The TAL and LAL parameters are used to limit the number of accesses to the encrypted data (e.g., The LAL parameter serves as a counter and is decremented after each access. When it reaches zero, access is disabled). *Id.* at col. 5, lines 61-67. When a packet is accessed, a key is obtained from the header and used to decrypt the encrypted body of data. *Id.* at Fig 5b. Once the data has been accessed, it is subsequently re-encrypted using the next key in the header. *Id.* at Fig 5b.

***

In the present Office Action, Examiner alleges that claim 156 is not patentably distinct over the cited references. Applicant respectfully submits that the cited references do not teach or suggest at least the following features of amended claim 156 (emphasis added):

> a first utilization permit key capable of use in cryptographic operations and ***configured to permit one or more of the following uses of digital data; displaying, editing, storing, copying, transferring****;* and
>
> a second utilization permit key capable of use in cryptographic operations and ***configured to permit one or more of the following uses of digital data: displaying, editing, storing, copying, transferring***, wherein one or more uses permitted by the second utilization permit key are different from the one or more uses permitted by the first utilization permit key; and
>
> decrypting encrypted digital data using the received one or more of the plurality of utilization permit keys that includes at least the first utilization permit key or the second utilization permit key for ***performance of only the use or uses of the digital data that are permitted by the received one or more utilization permit keys.***

The Examiner admits that "Shear does not expressly disclose permit keys that permit different types of uses of digital data comprising one or more of the following: display, edit, storage, copy, or transfer." *See* Office Action at 5.

Applicant submits that the other references cited by the Examiner also fail to teach the above-noted limitations of claim 156. Matyas, for example, is concerned only with "controlling the use of [the] cryptographic key," Matyas, abstract, lines 1-3, and not "decrypting encrypted digital data … *for performance of only the use or uses of the digital data that are permitted by the received one or more utilization permit keys*," as recited in claim 156 (emphasis added). As noted above, Sklut does not teach or suggest "decrypting encrypted digital data using the received one or more of the plurality of utilization permit keys" as recited in claim 156, as that reference is directed to a **<u>physical</u>** key. Finally, while Narasimahlu's "control header" contains parameters such as those limiting the number of times the body of data can be accessed, there is no teaching or suggestion of "decrypting encrypted digital data … *for performance of only the use or uses of the digital data that are permitted by the received one or more utilization permit keys*."

Accordingly, none of the cited references teach or suggest "decrypting encrypted digital data … for performance of only the use or uses of the digital data that are permitted by the received one or more utilization permit keys," as recited in claim 156. Accordingly, even if the references were combinable in the manner suggested by the Examiner (which Applicant definitely does not concede), the resulting combination would not teach each and every limitation of claim 156. As such, the Examiner has not established a *prima facie* case of obviousness. Claim 156 and its dependent claims are therefore believed to be patentably distinct over the cited references. The remaining independent claims are believed allowable, along with their respective dependent claims, for at least the reasons presented above in support of claim 156.

Applicant also directs the Examiner's attention to the response to Office Action in related U.S. Appl. No. 09/985,279, filed October 31, 2007.

CONCLUSION:

Applicants submit the application is in condition for allowance, and an early notice to that effect is requested.

If any extension of time (under 37 C.F.R. § 1.136) is necessary to prevent the above-referenced application from becoming abandoned, Applicant hereby petitions for such extension.

The Commissioner is authorized to charge any fees that may be required, or credit any overpayment, to Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C. Deposit Account No. 501505/6057-46717/DMM.

Respectfully submitted,

Date: October 31, 2007

By: /Dean M. Munyon/
Dean M. Munyon
Reg. No. 42,914

Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C.
P. O. Box 398
Austin, Texas 78767
(512) 853-8847